

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-040100

(43)Date of publication of application : 13.02.1998

(51)Int.Cl.

G06F 9/06
G06F 13/00
G06F 15/00
G06F 17/60
G09C 1/00
H04L 9/08
H04L 9/14

(21)Application number : 09-071388

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(22)Date of filing : 25.03.1997

(72)Inventor : AUERBACH JOSHUA SETH
CHOW CHEE-SENG
KAPLAN MARC ADAM
CRIGLER JEFFREY CHARLES

(30)Priority

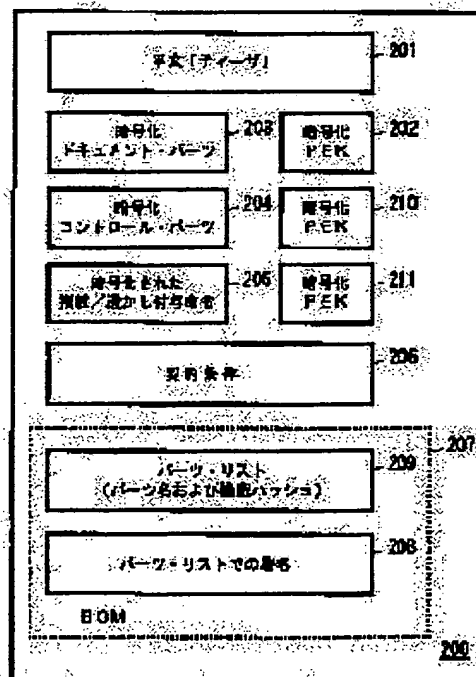
Priority number : 96 625475 Priority date : 29.03.1996 Priority country : US

(54) METHOD FOR PREPARING CIPHER ENVELOPE

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a method for preparing, distributing, and vending a digital document, and a method for managing access to the digital document by providing a step for enciphering one of information parts by a part enciphering key, and preparing an enciphered part to be housed in an envelope.

SOLUTION: A document part 203 can be enciphered. The enciphered document part 203 can be a 'valuable content' (for example, the chapter of a book, high resolution JPEG picture, or MPEG stream) to be purchased by a user. A non-enciphered part is a 'thesis' (for example, a book review by the others, index, summarization, or low resolution JPEG picture). The purpose of the non-enciphered part is to allow the user to attain the 'preview', 'sampling' or 'browse' of the content of the enciphered envelope before actually purchasing it.



LEGAL STATUS

[Date of request for examination] 30.07.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3130267

[Date of registration] 17.11.2000

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-40100

(43) 公開日 平成10年(1998) 2月13日

| (51) Int.Cl. ⁶ | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
|--------------------------------------|-------|----------|---------------|---------|
| G 0 6 F 9/06 | 5 5 0 | | G 0 6 F 9/06 | 5 5 0 Z |
| | 13/00 | 3 5 1 | | 3 5 1 G |
| | 15/00 | 3 3 0 | | 3 3 0 Z |
| | 17/60 | 7259-5 J | G 0 9 C 1/00 | 6 6 0 E |
| G 0 9 C 1/00 | 6 6 0 | | G 0 6 F 15/21 | Z |
| 審査請求 未請求 請求項の数 8 O L (全 13 頁) 最終頁に続く | | | | |

(21) 出願番号 特願平9-71388

(22) 出願日 平成9年(1997) 3月25日

(31) 優先権主張番号 08/625475

(32) 優先日 1996年3月29日

(33) 優先権主張国 米国 (US)

(71) 出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州
アーモンク (番地なし)

(72) 発明者 ジョシュア・セス・オーバック

アメリカ合衆国06877 コネチカット州リ
ッジフィールド ホルムズ・ロード 129

(74) 代理人 弁理士 合田 潔 (外2名)

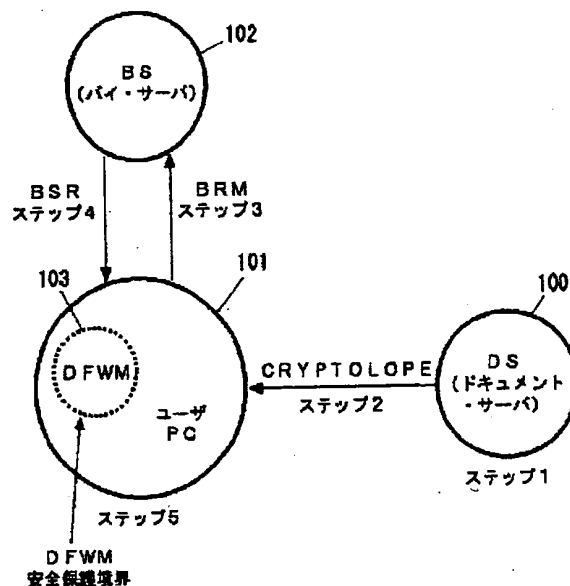
最終頁に続く

(54) 【発明の名称】 暗号エンベロープの作成方法

(57) 【要約】

【課題】 安全な暗号エンベロープを使用して、デジタル文書を作成し、配布し、販売し、アクセス管理を行う方法および装置。

【解決手段】 エンベロープは情報パーツの集合体であり、保護されるべきパーツの各々に対応するパーツ暗号化キーによって暗号化され、エンベロープの一部となる。各パーツ暗号化キーも公開キーによって暗号化され、エンベロープに収められる。エンベロープは各エントリがパーツ名と命名されたパーツの機密ハッシュを有しているパーツのリストも含んでいる。このリストは次いで、秘密キーによって署名されて、これもエンベロープに収められる署名を生成する。第1の秘密キーに関連づけられた第2の公開キーを使用して、署名を検証することができ、エンベロープ内の情報パーツの完全性は第2のハッシュを計算し、これをパーツのリストの対応するハッシュと比較することによって調べられる。



【 特許請求の範囲】

【 請求項1 】 複数のユーザに任意に配布でき、情報パーツの集合体であるデジタル文書である暗号エンベロープを作成する方法において、

a . 前記情報パーツの1 つをパーツ暗号化キーによって暗号化して、前記エンベロープに収められる暗号化パーツを作成するステップと、

b . 前記パーツ暗号化キーを第1 の公開キーによって暗号化して、前記暗号エンベロープに収められる暗号化パーツ暗号化キーを作成するステップと、

c . 前記エンベロープに収められているパーツのリストであって、該リストの各エントリがパーツ名と該命名パーツの機密ハッシュとを含んでおり、該リストも前記エンベロープに収められるパーツのリストを作成するステップと、

d . 前記リストに第1 の秘密キーによって署名して、前記エンベロープに収められる署名を作成するステップとを備えており、

前記リストの完全性を前記第1 の秘密キーに関連づけられた第2 の公開キーによって調べて、前記署名を検証することができ、前記エンベロープのいずれか1 つのパーツの完全性を該1 つのパーツの第2 の機密ハッシュを計算し、かつ該第2 のハッシュを前記リスト内の対応するハッシュと比較することによって調べることができ、前記暗号エンベロープの情報コンテンツが開示から保護され、前記パーツ暗号化キーによってのみ復元することができ、前記パーツ暗号化キーが前記第1 の公開キーに対応する第2 の秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読することによってのみ復元できる、暗号エンベロープを作成する方法。

【 請求項2 】 前記文書の前記パーツから選択したものを、この選択したパーツ内の選択したワードまたはビットの挿入、削除または変更により修正し、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報を維持するステップをさらに含んでいる、請求項1 に記載の方法。

【 請求項3 】 前記パーツの前記暗号化前に、前記修正を前記パーツから選択したものに適用し、第3 の公開キーによって暗号化される第3 のパーツ暗号化キーを使用して、前記状態情報を暗号化する、請求項2 に記載の方法。

【 請求項4 】 前記暗号エンベロープが、サーバで実行されるものであるコンピュータ・プログラムを含んでおり、前記実行の結果が前記サーバによる以降の操作を決定する、請求項1 に記載の方法。

【 請求項5 】 前記プログラムが前記暗号エンベロープ内の前記情報パーツのアクセスに関する契約条件を記述しており、前記実行が前記情報パーツへのアクセスが許可されるかどうかを決定する、請求項4 に記載の方法。

【 請求項6 】 前記プログラムが各情報パーツを修正する

命令を含んでおり、各パーツが各パーツ内の選択したワードまたはビットの挿入、削除、または変更によって修正され、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報が維持される、請求項4 に記載の方法。

【 請求項7 】 暗号エンベロープ内のコンテンツ・データへのアクセスをもたらす方法において、

a . 前記暗号エンベロープのパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求をユーザからのサーバに伝送するステップと、

b . 前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送するステップとを備えており、前記変形物が前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、

第2 の公開キーを使用して前記パーツ暗号化キーを暗号化し、

20 前記変形化キーを前記秘密キーを使用して、前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。

【 請求項8 】 複数の端末装置へ電子的にアクセスするサーバを有する通信ネットワークにおいて、選択したコンテンツ・データへのアクセスを与える方法において、前記暗号エンベロープが

a . 複数のユーザに任意に配布でき、情報パーツの集合体であるデジタル文書である暗号エンベロープを作成することによって生成され、該生成方法が

(i) その1 つが前記の選択したコンテンツ・データを含んでいる、保護されるべき前記パーツの各々にパーツ暗号化キーに関連づけ、

(i i) 保護されるべき前記パーツの各々をこれに関連したパーツ暗号化キーによって暗号化し、

(i i i) 前記の各パーツ暗号化キーを公開キーによって暗号化して、前記パーツ暗号化キーの各々に対する暗号化パーツ暗号化キーを形成し、

40 (i v) 各エントリが前記パーツの1 つに対するパーツ名と該1 つのパーツに対する機密ハッシュとを含んでいるパーツのリストを作成し、

(v) 前記リストに秘密キーによって署名して、署名を作成することからなっており、前記暗号エンベロープが前記署名、前記リスト、前記暗号化パーツ暗号化キー、前記暗号化パーツ、および前記情報パーツのうち暗号化されていないものの集合体であり、

b . 前記暗号エンベロープのコピーを所有しているユーザが前記の選択したコンテンツ・データにアクセスすることを希望した場合に、

(i) 前記暗号エンベロープの前記の選択したコンテンツ・データを含んでいるパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求を前記ユーザからサーバへ伝送し、

(i i) 前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送することによって前記アクセスが与えられ、前記変形物がステップb (i) の前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、

第2の公開キーを使用して前記要求の前記パーツ暗号化キーを暗号化し、

前記変形化キーを前記秘密キーを使用して、前記要求の前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。

【 発明の詳細な説明】

【 0001 】

【 発明の属する技術分野】 本発明は安全な暗号エンベロープの方法および技法を使用したデジタル文書の作成、配布、および販売方法、ならびにデジタル文書へのアクセスの管理を記載する。

【 0002 】

【 従来の技術】 デジタル文書は紙ベースのアナログ文書を凌駕するさまざまな利点を有している。これらの文書は作成、配布および複製が容易である。しかしながら、これらの利点はこれらの文書に関連した知的所有権を侵害から守ることを困難とする。それにもかかわらず、デジタル文書は将来の情報の配布および販売手段として紙ベースの文書に置き換わっていくであろう。

【 0003 】

【 発明が解決しようとする課題】

CD-Showcase (米国特許第5319705号)

本発明とCD-Showcase 特許[2]との重要な違いは、部分暗号キーが暗号エンベロープに収められており、公開キーで暗号化されるところにある。これに対し、CD-Showcase では、配布データが暗号キーの識別子を含んでいるだけである。暗号キーはサーバに記憶されており、キーの識別子が提示されたときに検索される。

【 0004 】 したがって、CD-Showcase 特許では、キー・データベースをサーバに維持しておく必要があり、バイ・サーバとドキュメント・サーバとの間の信頼性に関する対策を必要とする。

【 0005 】 PGP (Pretty Good Privacy)

PGP [3] は安全な電子メールを送るための公開キー・ベースのシステムである。電子メールの本文はID E

Aアルゴリズム (たとえば、[1] 参照) を使用して暗号化され、暗号キーは予定している受信者の公開キーを使用して暗号化される。暗号化された電子メールのテキストと暗号化された暗号キーの両方が送られる。受信者は自分の秘密キーを使って、暗号キーを復元し、この暗号キーは平文のテキストを復元するために使用される。

【 0006 】

【 課題を解決するための手段】 本発明は安全な暗号エンベロープの方法および技法を使用したデジタル文書の作成、配布、および販売方法、ならびにデジタル文書へのアクセスの管理を説明する。暗号エンベロープは最新の暗号化技法 (暗号化および認証などの) を使用して、文書部分を無許可の読取りや改竄に対して安全なものとする。

【 0007 】 本明細書で説明するプロセスにより、暗号エンベロープのパーツをユーザが購入し、ユーザの情報内容を安全で管理された態様で公開することが可能となる。パーツをさらに処理して、海賊行為を防止する。さらに、公開キー技法を使用することにより、暗号エンベロープ技法がデジタル情報を配布する便利で、安全で独立した手段となる。

【 0008 】 スーパー・ディストリビューション 本明細書で想定している情報配布の基本モデルは「スーパー・ディストリビューション」である (この詳細については、[5] 参照)。基本的な考え方は、各デジタル文書が「暗号化」されている限り、この文書 (または、「パーツ」) をインターネットにより、無線またはテレビジョン信号により、ケーブルにより、人工衛星により、ローカル・エリア・ネットワークにより、ディスクットにより、CD-ROMにより、BBSにより自由に配布できるということである。「暗号化プロセスが十分安全なものであるとすると」、ユーザがコンテンツにアクセスできる唯一の方法は、必要なPEK (パーツ暗号キー: part encryptionkey) を購入することである。このキーは通常、ユーザが暗号解読する文書よりも数桁コンパクトなものである。

【 0009 】 スーパー・ディストリビューションは情報配布の問題を、(1) バルク・データの配布と、(2) PEKの公開によるコンテンツの管理された公開とに分割しているため、強力な概念である。

【 0010 】 本発明はこの基本的な概念を拡張し、コンテンツの配布および販売に暗号エンベロープの技法を導入する。さらに、これらの概念と技法を一般化して、デジタル文書へのアクセスおよびその使用に関する「契約条件」を取り扱う。一般化することによって、暗号エンベロープをデジタル文書の分散アクセス監理の設計および実施の基礎として使用することが可能となる。

【 0011 】 本発明はこのようなキー・データベースをサーバに維持することを不必要とし、さらにドキュメント・サーバ (コンテンツが暗号化されるところ) とバイ

・サーバ(文書暗号キーを取得できるところ)とをきれいに分離することを可能とする。

【0012】したがって、本発明は任意の数のユーザに任意に配布できるが、機密情報パーツの平文テキスト内容にアクセスできるのは許可を受けたユーザだけである暗号エンベロープを作成する方法を提供する。本発明では、情報パーツの各々を対応するパーツ暗号キーによって暗号化して、暗号化情報パーツを生成する。各パーツ暗号キーを次いで、公開キーによって暗号化する。エンベロープに収められたパーツのリストも作成され、リストの各エントリはパーツ名と個々のパーツの機密ハッシュを有している。この場合、エンベロープは暗号化情報パーツ、暗号解読済み情報パーツ、暗号化パーツ暗号キーおよびパーツのリストを含んでいる。さらに、パーツのリストには署名を作成するために秘密キーによって署名がなされる。この署名もエンベロープに収められる。リストの完全性はリストの署名に使用された秘密キーに関連づけられた第2の公開キーを使ってチェックできる。任意の情報パーツの完全性はパーツの第2のハッシュを計算し、第2のハッシュをリスト内のそのパーツの対応するハッシュと比較することによってチェックできる。さらに、暗号化されたパーツの情報コンテンツは開示に対して保護され、これを復元できるのはパーツ暗号キーだけである。公開キーに対応した機密に関する知識は、暗号解読済みのパーツ暗号キーから取得する必要がある。次に、この暗号解読済みパーツ暗号キーが、情報パーツから平文テキストを生成するために使用される。

【0013】

【発明の実施の形態】図1を参照すると、暗号エンベロープの主要な利点の1つは安全保護である。BS(バイ・サーバ)102およびDS(ドキュメント・サーバ)100が安全なものとする。たとえば、これらは企業内のそれぞれのビジネス・パートナーによって管理され、所有されており、コンピュータ室内の信頼できる人間によって運用される。

【0014】また、UPC(ユーザのパーソナル・コンピュータ)101はユーザに属するものであるから、安全保護がソフトウェアや改竄防止ハードウェアによって与えられる比較的小規模で、安全なDFWM(Decryption Fingerprinting and Watermarking Module: 暗号解読指紋/透かし付与モジュール)103があることを除けば、十分な安全保護がないものとする。

【0015】ステップの概要処理ステップの概要は以下の通りである(図1参照)。

【0016】ステップ1. 暗号エンベロープの作成

ステップ2. 暗号エンベロープの配布

ステップ3. ユーザが行う購入要求

ステップ4. バイ・サーバの応答

ステップ5. 暗号エンベロープの開封

【0017】暗号エンベロープ処理ステップ

これらの処理ステップの各々を以下で詳細に説明する。

【0018】ステップ1. 暗号エンベロープの作成

最初のステップは暗号エンベロープの作成である。図2の200参照。作成事象はスーパー・ディストリビューションすべきデジタル文書を集める必要があると考えられるため、通常、コンテンツ・プロバイダによってオフラインで行われる。

【0019】あるいは、これをユーザの要請で開始してもよい。この場合には、暗号エンベロープが特にこのユーザのために作成されることとなり、暗号エンベロープはそのユーザあるいは要請に固有な情報を含んでいてもよい。さらに、他のユーザから将来同様な要請があると予想される場合には、付加的な情報を暗号エンベロープに含め、暗号エンベロープを「キャッシュ」して、将来の類似した要請を効率よく満たすようにすることもできる。

【0020】暗号エンベロープのパーツ

暗号エンベロープは「情報パーツ」をグループ化したものである。図2の201-211参照。情報パーツの中には暗号化されたものも、平文テキストのものもある。暗号エンベロープ・プロセスは広範囲にわたるグループ化技術(zip, tar およびOpenDoc Bent oやマイクロソフトOLEなどのオブジェクト指向度の高い手法)と両立する。グループ化方法の要件は最小限である。(1) パーツを配布に適したユニットにまとめ、パーツを後で個別に検索できるようにする、(2) さまざまなパーツを、たとえば、命名、ポインタ、あるいは索引などで関連づける手段がなければならない。

【0021】情報パーツには2つのタイプ、すなわち「ドキュメント」(201および203)と、「コントロール」(202、204-211)がある。ドキュメント・パーツは「コンテンツ」である。ドキュメント・パーツの例としては、要約、目次、図、表、および本文などがある。これらは、実行可能プログラム、サブルーチン・ライブラリ、ソフトウェア・モジュール、あるいはオブジェクト・コンポーネントの一部となることもできる。

【0022】図2を参照すると、ドキュメント・パーツは暗号化することができる(203)。暗号化ドキュメント・パーツ203はユーザが購入する「価値のあるコンテンツ」(たとえば、書物の章、高解像度PEGビクチャ、あるいはMP EGストリーム)であることがしばしばある。未暗号化パーツは「ティーザ」201(たとえば、他人による書評、目次、要約、または低解像度PEGビクチャ)である。未暗号化パーツの目的はユーザがユーザが実際に購入する前に、暗号エンベロープの内容の「プレビュー」、「サンプリング」、または「ブラウズ」を行えるようにすることである。

【0023】特別なストリング・パターンの圧縮および挿入などの前処理の中には、ドキュメント・パーツに適

用されるものもある。圧縮は記憶域を削減する。他の前処理はDFWMによるドキュメント・パーツの指紋／透かし付与を容易とするためのドキュメント・パーツに対する改変である。

【0024】コントロール・パーツは暗号エンベロープの機能およびプロセス・モデルをサポートするのに必要なメタデータである。2つの主要機能、「真性性」と「秘密性」がある。暗号エンベロープでこれらは改竄されない。この認証機能はデジタル署名を使用して達成される。秘密性機能は暗号化(たとえば、DESまたはIDEAを使用した)によって達成される。これらの暗号化および認証技法の基礎となるものは当分野で周知であり、暗号に関する新しいどの文献にも載っている(たとえば、[1]参照)。すべてのコントロール・パーツは認証を受けるし、また、必要に応じて、暗号化されるものもある。

【0025】コントロール・パーツの例としては価格マトリックス(図4の400参照)や、ドキュメント・パーツの後処理用の指紋／透かし付与命令205がある。ドキュメント・パーツの後処理は、暗号エンベロープが開かれたときに、DFWMによって行われる。指紋／透かし付与は後処理の例であり、ドキュメント・パーツに何らかの態様でマークを付けて、海賊行為を防止する。

【0026】図4を参照する。価格マトリックス400はドキュメント・パーツの購入に関する価格構造、たとえば、複数部購入時の数量割引、会員割引、または企業割引を記述している。式の例401はn部の文書の購入価格を計算するものである。(注: 価格割引率は時間によって変動するものであってもよく、その場合には、価格マトリックスの列(402-405)は会員ではなく、期間限定の特別価格となる。)

【0027】図2を参照すると、ドキュメント・パーツの購入および使用に関する契約条件206も暗号エンベロープに含まれている。これらはドキュメント・パーツ(この場合には、ユーザに可視となる)として含まれていても、あるいはコントロール・パーツ(この場合には、バイ・サーバ(BS)102で評価され、またおそらくはユーザのパーソナル・コンピュータ(UPC)101でも評価される)として含まれていてもよい。ドキュメント・パーツは契約条件を実現する何らかのプログラム(たとえば、Perl[4]などのスクリプト言語で書かれた)を含んでいてもよい。(注: 指紋／透かし付与命令と価格マトリックス。明確とするため、これらを明示的にリストする。)

【0028】秘密性および真性性

秘密性を達成することのできる方法をここで説明する。価値の一部はDES(データ暗号化規格)アルゴリズム(たとえば、[1]参照)を使用して暗号化される。異なるパーツは異なるPEK(パーツ暗号化キー)を使用して暗号化される。これらのキーはランダムに、かつ独

立して選択される。

【0029】ランダム暗号化キーを生成するには、多くの方法がある。1つの方法は乱数発生器または疑似乱数発生器を使用して、キーとして使用されるランダム・ストリングを作成することである。この手法の詳細については、[1, 3]を参照されたい。

【0030】各PEKはBS(バイ・サーバ)102の公開キーを使用して暗号化され、得られる暗号化PEK202(図2)は暗号エンベロープのコントロール・パーツとなる。(注: PEKを異なるBS公開キーを使用して暗号化することができ、これらすべての暗号化されたPEKは暗号エンベロープに含まれる。)

【0031】暗号エンベロープおよびそのパーツの真性性を確認するには、多くの方法がある。このような方法の1つをここで説明する。すべての暗号エンベロープはBOM(部品表)207という特別なコントロール・パーツを有している。BOMは2つの部分、(1)パーツ・リスト209と(2)デジタル署名208からなっている。

【0032】機密ハッシュ機能MessageDigest5(MD5)(詳細については、[1]参照)を、暗号エンベロープに含まれている各パーツに適用し、リストを作成する。図3を参照すると、リストの各エントリはパーツ名すなわち参照302と、パーツ名に対応した情報パーツの機密ハッシュ301を含んでいる。(たとえば、ファイル・ベースのグループ化の場合、パーツ・リストはすべてのファイルのファイル名とこれらの対応するハッシュ結果を含むものとなる。)

【0033】次いで、リストにはDS(ドキュメント・サーバ)100だけにわかる秘密キーによってデジタル署名がされる。文書にデジタル署名を行うには多くの方法がある(たとえば、[1]参照)。1つの方法はパーツ・リストのMD5(または、その他の機密ハッシュ)を計算し、得られるハッシュを秘密キー(「署名」を作成する)208を使用して暗号化することである。パーツ・リストおよび署名をまとめてBOM207という。BOMの真性性を検査するのに必要なのは、DSの公開キーだけである。

【0034】暗号エンベロープの真性性はDSの公開キーを使用して署名を暗号解読し、これをパーツ・リストのMD5と比較することによって調べられる。2つが合致すれば、パーツ・リストは改竄されていないことになる。個々のパーツの真性性も各パーツのMD5を計算し、その結果をリストの対応するエントリと比較することによって調べることができる。したがって、BOM207は暗号エンベロープとそのすべてのパーツの完全性を保証するものである。

【0035】独立した暗号エンベロープ
暗号エンベロープの重要な特徴はこれが以下の意味で独立していることである。暗号エンベロープの真性性を検

10

20

30

40

50

査するのに必要なのは、DSの公開キーだけである。暗号化PEK(202、210、211。図2参照)が暗号エンベロープに付随しているため、内容を復元するのに必要なのは、BSの秘密キーだけである。さらに、異なるドキュメント・サーバはBSの公開キーだけを使用して暗号エンベロープを生成することができ、BSとDSの間の他の通信は必要ない。

【0036】暗号エンベロープ作成ステップ

暗号エンベロープの作成時の処理ステップをまとめると、次のようになる(図2参照)。

【0037】1-a。暗号エンベロープに含める情報パーツをアSEMBルする。

【0038】1-b。オプションの処理ステップ(たとえば、圧縮、事前指紋/事前透かし付加)をパーツに適用する。後で操作やり直すため、これらの処理ステップの十分な状態情報を維持しておく。

【0039】1-c。暗号化対象の各パーツに1つ、ランダムなPEK(パーツ暗号化キー)を生成する。

【0040】1-d。ドキュメント・パーツをそれぞれのPEKによって暗号化して、暗号エンベロープに含められる暗号化されたパーツ(203、204、205)を形成する。

【0041】1-e。次に、BSの公開キーを使用して、PEKを暗号化して、暗号エンベロープに含められる暗号化PEK(202、210、211)を形成する。暗号化PEKおよびその対応する暗号化パーツは関連づけられる。

【0042】1-f。また、何らかのランダムPEKを使用して、処理ステップ1-bの命令およびその他の状態情報を暗号化する。PEKはBSの公開キーによって暗号化される。暗号化パーツ(203、204、205)および暗号化PEK(202、210、211)は両方とも暗号エンベロープに収められる。

【0043】1-g。暗号エンベロープに、「ティーザ」、概要および目次などの平文テキスト201を収める。

【0044】1-h。指紋/透かし付与命令205や価格マトリックス206などの契約条件を収める。必要に応じ、パーツやサブパーツを暗号化する(そして、これらの暗号化PEKを収める)。前述のように、暗号化パーツをその暗号化PEKと関連づける。

【0045】1-i。アSEMBルしたすべてのパーツをリストし、リストされたパーツの各々に対して機密ハッシュを計算して、情報パーツのリスト209を作成する。

【0046】1-j。リストにデジタル署名を行うことによって、たとえば、リストの機密ハッシュを計算し、これをDS秘密キーによって暗号化することによってBOM207に対する署名208を作成する。BOM207(リスト209および署名208)を暗号エンベ

ロープに加える。

【0047】考えられる暗号エンベロープの構造の詳細については、図2を参照されたい。

【0048】ステップ2。暗号エンベロープの配布

暗号エンベロープが作成されると、これを任意の手段、たとえばインターネットで送信することによって、無線またはテレビジョン信号によって、有線で、人工衛星によって、CD-ROMによって、あるいはBSによって配布することができる。配布の安全保護は必要ない。

10 暗号エンベロープをコピーしたり、複製を作ったり、あるいはユーザ間で共有したりすることができる。実際には、本発明者らが期待しているのは、暗号エンベロープの「下流」での配布(すなわち、友人同士が暗号化エンベロープをコピーすること)が暗号エンベロープを配布する費用効果の高い手段となることである。最後に、暗号エンベロープは任意のサーバの格納することができ、サーバにはいかなるセキュリティ要件もない。

【0049】ステップ3。ユーザが行う購入要求

このステップは暗号エンベロープの平文の「ティーザ」部分201を閲覧したユーザによって行われることがしばしばある。暗号エンベロープの内容に関心を持ったユーザは必要なPEKをBSから購入しなければならない(図1参照)。

【0050】グラフィカル・ユーザ・インタフェース

暗号エンベロープの閲覧は暗号エンベロープの構造を理解している修正ウェブ・ブラウザなどのGUIの助けを借りて行われる。まず、修正ブラウザは暗号エンベロープの完全性を調べる必要がある。ユーザには完全性チェックにより暗号エンベロープの改竄が通知される。次に、ブラウザは暗号エンベロープの平文テキストを表示する、たとえば概要と目次を表示できなければならない。最後に、図2および図5を参照すると、ブラウザは暗号エンベロープ200から、BRM(購入要求メッセージ)500を構築するのに必要なパーツを抽出できなければならない。

【0051】事前登録

ユーザがBSによって認識されるように、事前登録ステップをユーザが行っているものと想定している。たとえば、ユーザは信頼できるサード・パーティに登録することができる。

【0052】たとえば、登録はユーザが登録センタに電話をかけ、センタがユーザに対してアカウント番号を発行することを含んでいることができる。アカウント番号は次いで、すべてのBSに送られる。あるいは、登録センタはアカウント番号にデジタル署名を行うことができ、この場合には、BSでの更新は必要ない。BSは署名を調べることによってアカウント番号を検査するだけである。

【0053】登録後、ユーザにはある種の証明書(たとえば、アカウント番号その他の会員情報)が発行され

る。「証明書」は信頼できるサード・パーティがデジタル署名した文書であり、アカウント番号、所属、あるいはユーザが保持している権利などの情報も含んでいる。たとえば、サード・パーティがユーザに対して、表示価格からの割引を受ける権利をユーザに与えるある種の「ブック・クラブ」証明書を発行することができる。

【0054】機密DFWM

本方法に固有なものとして、登録に結果として、機密DFWM(図1の103)(暗号解読指紋透かし付与モジュール)の裏付けがUPCで行われるものと想定していることがある。

【0055】DFWMはパーツの暗号解読を行い、同時に、暗号解読済みパーツに指紋／透かし付与を適用することを担っている。透かし付与は消去が困難であるが、文書の閲読に影響を及ぼさないような態様で、可視のマークを付ける。指紋付与は文書の「不可視」のマークを付けることであり、したがって、除去が困難である。

【0056】指紋／透かし付与技法の詳細については1995年6月23日出願の米国特許願第08/494615号を参照されたい。

【0057】DFWMの裏付け

機密DFWMにはさまざまな実施形態がある。最も簡単なものは公開キー技法に基づくものであって、DFWMが秘密キーを機密に生成し、これをDFWM機密境界内に格納するものである。たとえば、DFWMは疑似乱数発生器を使用して、公開秘密キー対を作成することができる。DFWM秘密キーはDFWM内に格納され、公開キーは外部に公開される。登録プロセスによって、信頼できるサード・パーティがDFWM公開キーを証明することができるようになる(公開キーの証明プロセスについては、[1]参照)。DFWM秘密キーはDFWMモジュールの唯一の秘密情報である。

【0058】DFWMのセキュリティ

DFWMは物理的に安全なモジュール(たとえば、スマート・カード)で動作している、あるいはUPC環境(安全ではない)で動作しているソフトウェアの一部である。前者の場合、セキュリティはパッケージの物理的改竄防止策によって達成される。現在のパッケージング技術はすべての実用上の目的でDFWMに十分なセキュリティを与えることができる。

【0059】後者の場合、すなわち、DFWMの物理的セキュリティを想定していない場合に説明を絞る。この場合の方が興味深いのは、物理的セキュリティが利用できることはDFWMのセキュリティを橋架するだけのものだからである。

【0060】安全なハードウェアがなければ、DFWMのセキュリティを保証することができない。実用上多くの場合に、周知のソフトウェア技法(たとえば、ウィルスの作成者に周知のコード隠滅技法)を使用して、十分なセキュリティを達成できる。

【0061】しかしながら、本開示で記載するプロセスの主な利点の1つは、DFWMが危険にさらされたとしても、エクスポージャが限定されることである。ユーザは購入していないドキュメント・パーツのロックを解除することができない(PEKを利用できないため)。安全なBSを経由するため、購買トランザクションは安全である。

【0062】DFWMが危険にさらされた場合(たとえば、DFWMの秘密キーが暴露された場合)、考えられる損失はユーザが購入した文書に正しい指紋／透かし付与を行えないということだけとなる。しかしながら、セキュリティ・リスクはユーザが文書からマークを消去する可能性とまったく異なるというものではない。

【0063】購入要求トランザクション

ここで、購入要求トランザクションを詳細に説明する。

【0064】グラフィカル・ユーザ・インタフェース(GUI)により、ユーザには暗号エンベロープに収められている物品リストが表示される。ユーザは関連する概要を閲覧して、詳細な情報を得ることができる。ユーザは物品の表示価格を知ることできる。ユーザが物品の購入を希望する場合には、GUIによって購入要求を行い、BRM(購入要求メッセージ)(図5の500参照)がBS102へ送られることとなる。

【0065】ユーザの認証

購入要求を完全なものとする前に、システムがユーザの認証を行おうとすることもある。システムによるユーザの認証には多くの周知の方法がある。たとえば、このような技法の1つ(Pretty Good Privacy[3]で使用されているものと類似したもの)は、暗号化されたユーザの秘密キーをUPCのディスク装置に格納するものである。

【0066】ユーザはそのパスワードを入力するよう要求され、パスワードは秘密キーを暗号解読するために使用される。秘密キーはデジタル署名を行うか、あるいは購入関係のメッセージを確認するために使用され、各セッションの終了時に消去される。

【0067】環境変数

環境変数はユーザの環境に関する情報、またはUPCに関する情報(たとえば、場所、時間、機械タイプ、オペレーティング・システム名など)である。これとは対照的に、ユーザ証明書はユーザに関する情報である。

【0068】環境変数には2つのタイプ、すなわち「安全」および「非安全」がある。安全変数は検証され、デジタル署名される。これらをBSにより(登録中に)調べ、署名するか、あるいはDFWMによって生成して、署名するかのいずれかを行うことができる。

【0069】非安全変数はUPCによって生成される。これらは検証されず、また署名されない。これらは情報のためにのみ含まれる。本明細書全体にわたり、環境変数とはこれら両者を意味するものとする。

【0070】購入要求メッセージ

図5を参照すると、BRM500は暗号エンベロープ（図2の200）からコピーまたは抽出した次の情報を含んでいる。

【0071】3.1 暗号エンベロープ207のBOM

【0072】3.2 購入する物品リスト501

【0073】3.3 物品リストおよびその他の制御パーツ（202および211）に関連づけられたPEK

【0074】3.4 契約条件（価格マトリックスなど）206

【0075】また、ユーザ環境またはDFWMから、あるいはユーザがコピーまたは抽出した次の情報を含んでいる。

【0076】3.5 ユーザ証明書のリスト（たとえば、会員カードや割引カード）およびユーザ認証関連情報502

【0077】3.6 環境変数（たとえば、日時、場所、DFWMまたは機械のハードウェアID）503

【0078】3.7 DFWM公開キー504

【0079】暗号化および認証などの標準的な暗号技法をBRMに適用することもできる。BRMを認証する方法の1つはBRM全体のMD5を計算し、DFWMの秘密キーを使用して、得られるMD5を暗号化して、署名505を作成し、署名をBRMの末尾に追加することである。

【0080】BRMの生成までのステップをまとめると次のようになる。

【0081】3-a。GUIによる暗号エンベロープの平文部分の閲読。

【0082】3-b。購入する暗号エンベロープの情報の選択。

【0083】3-c。購入契約条件206（たとえば、表示価格、再販しない約束）に対するユーザによる明示的な同意。

【0084】3-d。認証のためのパスワードの入力のユーザに対する要求（その結果、ある種のユーザ認証関連情報が生成され、BRMに含められる）。

【0085】3-e。GUIによるBRM500の生成。

【0086】3-f。BSへのBRMの送信。

【0087】注：BRMを特別なタイプの暗号エンベロープ、すなわち「購入要求」暗号エンベロープと見なすことができる。

【0088】ステップ4。パイ・サーバの応答

BSR（パイ・サーバ応答）はBRMを受信すると送られる。BSRの送信前にBS（パイ・サーバ）が行う動作を詳細に説明する。

【0089】ユーザ口座

BSはBRMを受信すると、BOMを検証して、コントロール・パーツの真性を調べる。また、DFWM公開

キー、ユーザ証明書、およびユーザ認証関連情報の真性も調べる。ユーザは以前の登録ステップによりBSに口座を持っていることがあり、その場合には、該当する金額がユーザの口座から引き落とされる（ユーザが権利を持っている割引を適用した後）。

【0090】契約条件の評価

暗号エンベロープ（および、BRMに）に収められている契約条件206の主な目的は、購買を成立させるのに必要な、契約条件に記載されている要件をユーザが満たしていることを確認することである。BSは契約条件を評価（実行）することによって、ユーザが要件を満たしていることを調べる。評価の結果により、購買を完了できるかどうか判定される。結果が満足できるものであれば、他のステップが継続され、そうでない場合には、エラー・メッセージがBSRに入れられる。結果が満足できるものである場合、実購入価格も価格マトリックス（400）で与えられた式401を使用して計算される。

【0091】キーの変換

BRMでBSが行う動作の1つはキーの変換である。ステップ1で述べたように、PEK（パーツ暗号化キー）はBSの公開キーを使用して暗号化されている。BSはその秘密キーを使用してPEKを暗号解読する。暗号化PEKの暗号解読後、BSはDFWMの公開キーを使用して、PEKを再暗号化し、DFWMだけがPEKを復元できるようにする。これがキー変換ステップである。

【0092】指紋／透かし付与のカスタム化

BSが行う他の一連の動作は指紋／透かし付与命令のカスタム化である。ステップ1で述べたように、これらの命令はBS公開キーを使用して暗号化され、コントロール・パーツとして暗号エンベロープで搬送される。BSはまず命令を暗号解読し、次に、ユーザに関する情報（たとえば、ユーザ名、会員番号）およびトランザクションに関する情報（たとえば、購入日、ライセンスの限定事項、トランザクションID）を命令に含める。これらの命令は次いで、DFWM公開キーを使用して暗号化される。（DFWMはこれらの暗号化された指紋／透かし付与命令が存在していることを調べてから、文書を暗号解読する。）

【0093】契約条件の変換

コンテンツの使用に関する制限事項に関する他の態様が、BSRに含められる。BRMに収められている契約条件が強化されたり、修正されたりすることがある（たとえば、暗号エンベロープが作成されてから、契約条件が変更される）。結果として生じる契約条件は文書の使用に関する制限事項および契約条件を記載した簡単な平文テキストとなる。あるいは、契約条件を守らせる実行可能な命令、オブジェクト、およびエージェントであってもよい。これらはすべてBSRに収められている。

【0094】購入応答ステップ

図6を参照して、BRMの受信からBSRの送信までにBSが行うステップをまとめる。

【0095】4-a。BRMの受信

【0096】4-b。BRMの真性を調べ(BOMを調べるにより)、ユーザの証明書を検証し、ユーザの認証関連情報を検証し、DFWM公開キーを検証し、環境変数を調べる。

【0097】4-c。ユーザの証明書、価格マトリックス、および環境変数を入力(BRMからの)として、またデータベースにあるユーザ情報および付加的な環境変数を入力(BSからの)として使用して、契約条件を評価する。契約条件の評価からの出力は、(a)ユーザがパーツのアクセスすることを認められているかどうか、および(b)パーツ601を購入する実際の価格となる。

【0098】4-d。ユーザにアクセスが認められているかどうか、またユーザに十分な信用があるかどうかを調べる。そうでない場合には、異常終了し、エラーBSRを送信する。

【0099】4-e。PEKを変換する(BS秘密キーを使用してPEKを暗号解読し、DFWM公開キーを使用してPEKを再暗号化する)。これらをBSRに含める(602、603)。

【0100】4-f。指紋/透かし付与命令をカスタム化する。(命令を暗号解読し、ユーザ固有のトランザクション関連情報を命令に含める。DFWM公開キーを使用して、修正された命令を暗号化する。)これらをBSRに含める(604)。

【0101】4-g。文書の使用に関する変換された契約条件およびその他の制限事項をBSRに含める(605)。

【0102】4-h。BSRをユーザに送る。

【0103】BSRを特別なタイプの暗号エンベロープ、すなわち「ライセンス暗号エンベロープ」と見なすことができる。この場合も、暗号化および認証などの標準的な暗号技法を適用して、BSRのプライバシーと真性を保護することができる(606)(たとえば、[1]参照)。

【0104】ステップ5。暗号エンベロープの開封これは最終ステップである。このステップの前提条件は、BSからBSRを受け取っていることである。BSRの受信後、ユーザは都合のよいときに暗号エンベロープを開くことができる。

【0105】BSRは暗号エンベロープのロックを解除する「キー」である。PEKがすべてDFWM公開キーで暗号化されているため、BSRの内容を使用できるのは「特定」のDFWMだけである。図6を参照すると、暗号エンベロープの開封に関与するステップは次のようになる。

【0106】5-a。DFWMがBSRの真性を確認

するため、チェックを行う(606)。開封作業が継続されるのは、BSRの認証が成功した場合だけである。

【0107】5-b。ユーザに対して任意選択で、更新された契約条件605をBSRで求める。開封作業が継続されるのは、ユーザが契約条件に同意した場合だけである。

【0108】5-c。DFWMが変換されたPEK(602、603)とカスタム化された指紋/透かし付与命令(604)を認証し、暗号解読する。開封作業が継続されるのは、認証が成功した場合だけである。

【0109】5-d。暗号解読したPEKを使用して、DFWMが暗号エンベロープの対応する暗号化されたパーツを暗号解読する(203、205)。

【0110】5-e。DFWMが該当する指紋/透かし付与命令604を暗号解読した文書に適用する。(指紋/透かし付与はユーザに合わせてカスタム化され、無許可の配布をさらに防止する。)

【0111】5-f。得られる暗号解読された文書が、DFWMセキュリティ境界外のユーザに対して許可される。

【0112】暗号エンベロープのプロセスを、一般にきわめて機密性が高いデータ(患者の医療記録など)やデータベースに対して効率がよく、安全な分散アクセス管理を実施するために使用することもできる。

【0113】参考文献

1. B. Schneier, "Applied Cryptography, 2nd Edition," Addison Wesley, 1996.
2. IBM CD-Showcase 特許(1994年6月7日にB. Halter 他に対して発行された米国特許第5319705号)。
3. S. Garfinkel, "Pretty Good Privacy," O'Reilly & Associates, Inc., 1994.
4. L. W. WallおよびR. L. Schwartz, "Programming Perl," O'Reilly & Associates, Inc., 1991.
5. B. Cox, "Superdistribution and Electronic Objects," Dr. Dobbs' Journal, Vol. 17, No. 10, Oct. 1992.
6. 本出願人に譲渡された1995年6月23日出願の米国特許願第08/494615号「A METHOD TO DETECT R DOCUMENT AND INTELLECTUAL PROPERTY PRIVACY THROUGH INDIVIDUALIZATION」。

参考文献[1-6]は参照することにより、本明細書の一部となる。

【0114】まとめとして、本発明の構成に関して以下の事項を開示する。

【0115】(1)複数のユーザに任意に配布でき、情報パーツの集合体であるデジタル文書である暗号エンベロープを作成する方法において、

a. 前記情報パーツの1つをパーツ暗号化キーによって暗号化して、前記エンベロープに収められる暗号化パー

ツを作成するステップと、

b. 前記パーツ暗号化キーを第1の公開キーによって暗号化して、前記暗号エンベロープに収められる暗号化パーツ暗号化キーを作成するステップと、

c. 前記エンベロープに収められているパーツのリストであって、該リストの各エントリがパーツ名と該命名パーツの機密ハッシュとを含んでおり、該リストも前記エンベロープに収められるパーツのリストを作成するステップと、

d. 前記リストに第1の秘密キーによって署名して、前記エンベロープに収められる署名を作成するステップとを備えており、前記リストの完全性を前記第1の秘密キーに関連づけられた第2の公開キーによって調べて、前記署名を検証することができ、前記エンベロープのいずれか1つのパーツの完全性を該1つのパーツの第2の機密ハッシュを計算し、かつ該第2のハッシュを前記リスト内の対応するハッシュと比較することによって調べることができ、前記暗号エンベロープの情報コンテンツが開示から保護され、前記パーツ暗号化キーによってのみ復元することができ、前記パーツ暗号化キーが前記第1の公開キーに対応する第2の秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読することによってのみ復元できる、暗号エンベロープを作成する方法。

(2) 前記文書の前記パーツから選択したものを、この選択したパーツ内の選択したワードまたはビットの挿入、削除または変更により修正し、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報を維持するステップをさらに含んでいる、上記(1)に記載の方法。

(3) 前記パーツの前記暗号化前に、前記修正を前記パーツから選択したものに適用し、第3の公開キーによって暗号化される第3のパーツ暗号化キーを使用して、前記状態情報を暗号化する、上記(2)に記載の方法。

(4) 前記暗号エンベロープが、サーバで実行されるものであるコンピュータ・プログラムを含んでおり、前記実行の結果が前記サーバによる以降の操作を決定する、上記(1)に記載の方法。

(5) 前記プログラムが前記暗号エンベロープ内の前記情報パーツのアクセスに関する契約条件を記述しており、前記実行が前記情報パーツへのアクセスが許可されるかどうかを決定する、上記(4)に記載の方法。

(6) 前記プログラムが各情報パーツを修正する命令を含んでおり、各パーツが各パーツ内の選択したワードまたはビットの挿入、削除、または変更によって修正され、それぞれの未修正の文書を復元するために、修正した各ドキュメント・パーツをその修正に関連づける状態情報が維持される、上記(4)に記載の方法。

(7) 暗号エンベロープ内のコンテンツ・データへのアクセスをもたらす方法において、

a. 前記暗号エンベロープのパーツへのアクセス要求で

あり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求をユーザからのサーバに伝送するステップと、

b. 前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送するステップとを備えており、前記変形物が前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、第2の公開キーを使用して前記パーツ暗号化キーを暗号化し、前記変形化キーを前記秘密キーを使用して、前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。

(8) 複数の端末装置へ電子的にアクセスするサーバを有する通信ネットワークにおいて、選択したコンテンツ・データへのアクセスを与える方法において、前記暗号エンベロープが

a. 複数のユーザに任意に配布でき、情報パーツの集合体であるデジタル文書である暗号エンベロープを作成することによって生成され、該生成方法が(i)その1つが前記の選択したコンテンツ・データを含んでいる、保護されるべき前記パーツの各々にパーツ暗号化キーに関連づけ、(ii)保護されるべき前記パーツの各々をこれに関連したパーツ暗号化キーによって暗号化し、(iii)前記の各パーツ暗号化キーを公開キーによって暗号化して、前記パーツ暗号化キーの各々に対する暗号化パーツ暗号化キーを形成し、(iv)各エントリが前記パーツの1つに対するパーツ名と該1つのパーツに対する機密ハッシュとを含んでいるパーツのリストを作成し、(v)前記リストに秘密キーによって署名して、署名を作成することからなっており、前記暗号エンベロープが前記署名、前記リスト、前記暗号化パーツ暗号化キー、前記暗号化パーツ、および前記情報パーツのうち暗号化されていないものの集合体であり、

b. 前記暗号エンベロープのコピーを所有しているユーザが前記の選択したコンテンツ・データにアクセスすることを希望した場合に、(i)前記暗号エンベロープの前記の選択したコンテンツ・データを含んでいるパーツへのアクセス要求であり、前記パーツを暗号化するために使用されたキーの公開キー暗号化である暗号化パーツ暗号化キーを少なくとも含んでいる要求を前記ユーザからサーバへ伝送し、(ii)前記要求に応じて、前記サーバから前記ユーザへ、前記暗号化パーツ暗号化キーの変形物である応答を伝送することによって前記アクセスが与えられ、前記変形物がステップb(i)の前記公開キーに関連づけられた秘密キーを使用して前記暗号化パーツ暗号化キーを暗号解読し、第2の公開キーを使用して前記要求の前記パーツ暗号化キーを暗号化し、前記変

形化キーを前記秘密キーを使用して、前記要求の前記パーツ暗号化キーに暗号解読することによって生成され、前記の選択したパーツが前記パーツ暗号化キーを使用して平文テキストに暗号解読され、これによって前記ユーザにアクセスを与える前記方法。

【図面の簡単な説明】

【図1】暗号エンベロープ・プロセスの5つのステップの概要を示す図であり、このプロセスに関与する主なエントリがドキュメント・サーバ(DS)100、バイ・サーバ(BS)102、暗号解読指紋/透かし付与モジュール(DFWM)103、およびユーザのパーソナル・コンピュータ(UPC)101であることを示す図である。

【図2】典型的な暗号エンベロープの構造を示す図であり、最小限の要素が暗号化パーツ203、ならびにこれに関連した暗号化パーツ暗号キー(PEK)202、パーツ・リスト209、およびパーツ・リストの署名208であることを示す図である。

【図3】パーツ・リスト209を有する部品表(BOM)の構造を示す図である。表の各エントリはパーツ名302(たとえば、「Abstract」)、および個々のパーツのMessageDigest5(MD5)、すなわち機密ハッシュ301(たとえば、「13ADB77F...」)を含んでいる。リストのMD5が計算され、得られるハッシュにはDSの秘密キーを使用して署名がされ、デジタル署名208が作成される。リスト209および署名208がBOMを形成する。

【図4】典型的な価格マトリックスを示す図である。列

はさまざまな会員カテゴリ(402、403、404、405)に対する割引率を示し、行は数量割引(406、407、408、409)を示す。n部目の価格とn部の合計価格を計算する式の例は401に示すとおりである。

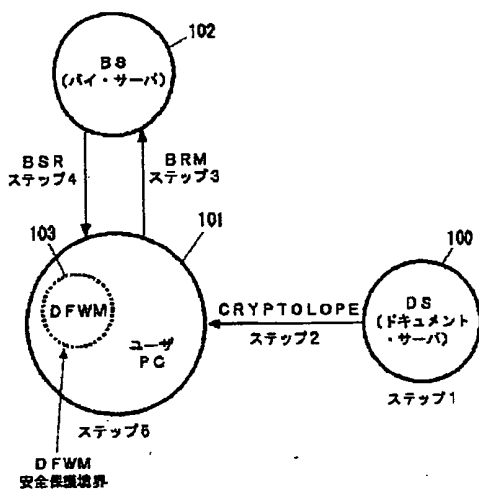
【図5】購入要求メッセージ(BRM)500を示す図である。BRMには、暗号化PEK(202、211)、暗号化指紋/透かし付与命令205、契約条件206、およびBOM207が含まれる。項目202、205、206、207および211は暗号エンベロープ200(図2参照)からコピーされる。BRMの他の部分(501-505)はUPCで生成される。

【図6】バイ・サーバ応答(BSR)600を示す。バイ・サーバ(BS)はPEKを変換して、DFWM103だけが暗号解読できる変換PEK(602、603)を作成する。指紋/透かし付与命令は暗号解読、カスタマイズ、および再暗号化され、その結果604を暗号解読できるのはDFWMだけとなる。BRM(500、図5)にある契約条件も評価され、更新または変換された契約条件605を作成する。実購入価格601は該当する割引を基本価格に適用することによって計算される。

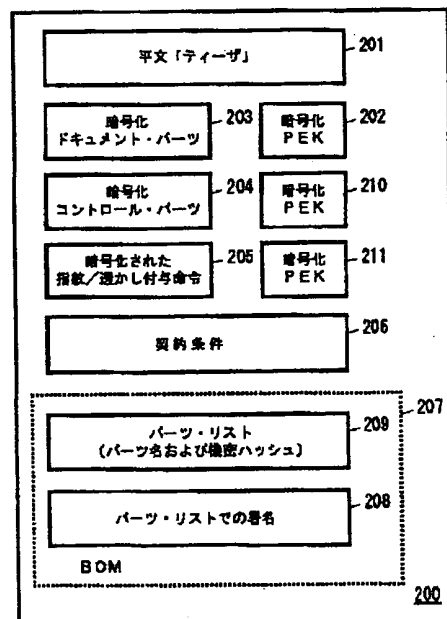
【符号の説明】

- 100 ドキュメント・サーバ(DS)
- 101 ユーザのパーソナル・コンピュータ(UPC)
- 102 バイ・サーバ(BS)
- 103 暗号解読指紋/透かし付与モジュール(DFWM)

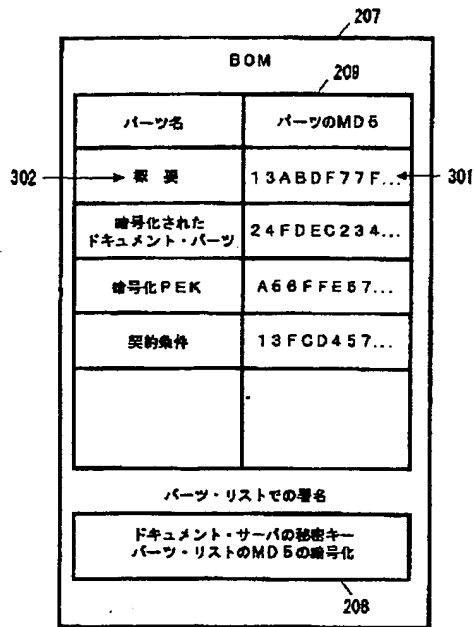
【図1】



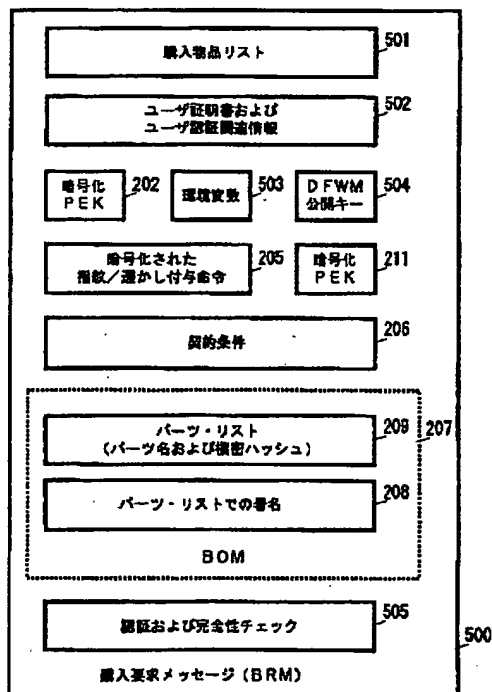
【図2】



【 図3 】



【 図5 】

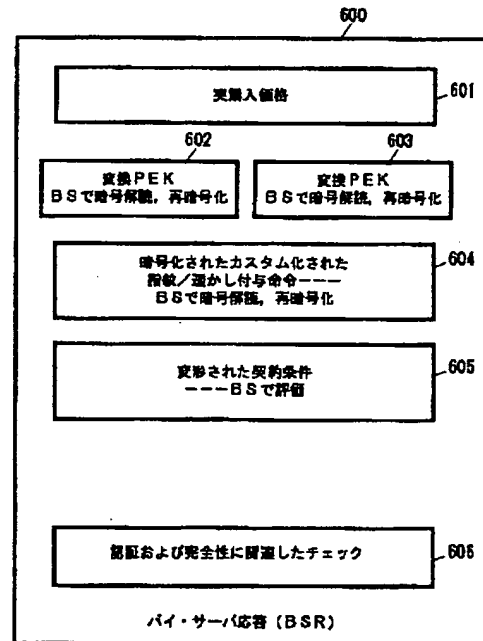


【 図4 】

| | 402 通常会員 | 403 企業割引 | 404 ゴールド・クラブ会員 | 405 プラチナ加入者 |
|----------------|-------------|-------------|-------------------|----------------|
| 400 | | | | |
| 406 1から10 | 1 | 0.8 | 0.8 | 0.75 |
| 407 11から50 | 0.9 | 0.8 | 0.8 | 0.75 |
| 408 51から100 | 0.85 | 0.75 | 0.7 | 0.75 |
| 409 100+ | 0.8 | 0.6 | 0.6 | 0.75 |

表示価格=¥2,500
 n 部目の価格=表示価格×最低適用割引率
 n 部目の価格=1 部目の価格+2 部目の価格+... n 部目の価格

【 図6 】



フロントページの続き

| (51) Int. Cl. ⁶ | 識別記号 | 庁内整理番号 | FI | 技術表示箇所 |
|----------------------------|------|--------|-----------|--------|
| H04L 9/08 | | | H04L 9/00 | 601A |
| 9/14 | | | | 641 |

(72)発明者 チー=セン・チョウ
アメリカ合衆国95014 カリフォルニア州
クパチーノ メイグス・レーン 19030

(72)発明者 マーク・アダム・カプラン
アメリカ合衆国10536 ニューヨーク州カ
トナーホーリー・ヒル・レーン 14
(72)発明者 ジェフリー・チャールズ・クリグラー
アメリカ合衆国 バージニア州マクリー
ディキシー・プレース 8601